Implementation Plan for the Department of Commerce
Significant Incident Coordination and Communication Process

The following process (pages 2 through 4) reflects the ideal steps for a smooth and orchestrated flow of activities and communications when the Department faces attack from significant IT events such as the recent SQL Slammer Worm. However, preliminary efforts are necessary to position the Department to implement such a process, including:

- Obtain agreement from all Departmental elements involved to follow the process.
- Establish criteria for what constitutes an incident advisory as a Significant Event within Commerce.
- Development and maintenance of a hierarchical significant event call roster. Uppermost would be a DOC Significant Event Action Alert call roster that would be maintained by the DOC CIRT and consist of one Operating Unit Significant Incident Contact person for each operating unit. This Contact would in turn maintain a call roster of system owners, system administrators, or others as appropriate to the operating unit's system environment.
- Determine the method, or methods, of contact – pager, e-mail, fax – that are appropriate in times of emergency.
- Establish operating unit and DOC CIRT procedures, including roles and responsibilities, to implement the process within all operating units.
- Finalize the Department's use of the Patch Authentication and Dissemination Capability (PADC) through the Federal Computer Incident Response Center (FedCIRC). This would include establishing all system profiles and sub-accounts within the Department's PADC database.
- Establish 24x7 coverage for the DOC CIRT. Opportunities exist for cost-sharing if this coverage will extend to notification beyond the Operating Unit Significant Incident Contact.

Department of Commerce
Significant Incident Coordination and Communication Process

Purpose

The occurrence of significant events of an urgent nature that affect systems within the Department's IT environment requires a process for timely, coordinated communication and specific action by Department of Commerce (DOC) personnel involved in computer incident response functions. This process provides an organized, managed flow of initial personnel notifications, actions to be taken and time frames for the actions, and confirmation responses that appropriate actions are complete.

Scope

This process will be followed by personnel involved in computer security incident response, including:

- Office of the Department's Chief Information Officer (CIO), to include the Critical Infrastructure Program Manager (CIPM) and the DOC Computer Incident Response Team (CIRT); and
- Operating Unit Significant Incident Contacts who may be CIOs, IT Security Officers, and formal CIRTs within DOC that support some operating units.

Process

Details of the process steps follow, and are depicted graphically in attachment 1.

Event (E)	The issuance of an incident advisory from the Federal Computer Incident Response Center (FedCIRC) triggers an event. All personnel on the FedCIRC mailing list receive the advisory, and each operating unit must have procedures documented and functioning to handle all FedCIRC advisories. The advisory will be followed by notification, from the Patch Authentication and Dissemination Capability (PADC) vendor to the CIPM (also the account manager for the Department's PADC agreement with FedCIRC), that the patch is available and has been authenticated.
E + 1 hr	Within 1 hour of issuance of the advisory from FedCIRC, the DOC Computer Incident Response Team (CIRT), staffed 24x7, notifies the CIPM who makes the determination that it is a Significant Event. The DOC CIRT begins work to enhance the advisory and develop a DOC Significant IT Event Action Alert. Enhancement includes researching all available data on the event and developing steps for preventing event from entering DOC IT infrastructure, restricting spread of event within DOC, and to eradicate event from affected DOC systems. The DOC CIRT will have the enhanced alert ready for distribution within 2 hours of the advisory issued by FedCIRC.
E + 2 hrs	The CIPM will query the PADC database to determine the DOC IT systems potentially affected by the event. Within 2 hours of the advisory issued by FedCIRC, the CIPM notifies the DOC CIRT of the affected operating units/systems.
E + 2 hrs	Upon notification from the CIPM, the DOC CIRT issues the enhanced action alert to the affected Operating Unit Significant Incident Contacts. The alert also

contains a request that Contacts update their respective PADC profiles and notify the DOC CIRT upon completion of corrective actions. This notification is issued within 2 hours of the advisory issued by FedCIRC.

E + 4 hrs Upon receipt of the DOC Significant IT Event Action Alert/data call from the DOC CIRT, the Operating Unit Significant Incident Contact notifies its formal CIRT (if applicable and other than the DOC CIRT), owners of affected systems, and system administrators. In addition, within 4 hours of the advisory issued by FedCIRC, the Contact accesses the PADC database, reviews affected system profiles, and downloads authenticated patches for the system administrators (or assists the system administrators to download patches from PADC or directly from the software vendor).

E + 12 hrs The corrective action implementer (e.g., the system administrator) obtains the authenticated patch from PADC or the software vendor. The implementer tests the patch on a development server or testbed, and installs the validated patch, and works with the DOC CIRT if difficulties arise with patch installation. Within 12 hours of the advisory issued by FedCIRC, the implementer notifies the Operating Unit Significant Incident Contact that corrective actions have been completed.

E + 16 hrs Upon notification from the implementer that the patches have been tested and installed, the Operating Unit Significant Incident Contact updates the PADC database for the affected systems and notifies the DOC CIRT that these actions are completed within 16 hours of the advisory issued by FedCIRC.

E + 20 hrs Upon notification from the Operating Unit Significant Incident Contact that the corrective actions are complete and the PADC database has been updated, the DOC CIRT performs scans to validate the effectiveness of the patch installation, and works with the operating unit Contact to resolve discrepancies. Within 20 hours of the advisory issued by FedCIRC, the DOC CIRT notifies the CIPM that corrective actions are complete and PADC is updated.

E + 24 hrs Upon notification from the DOC CIRT that corrective actions are complete and validated, the CIPM confirms information in the PADC database and works with the Operating Unit Significant Incident Contact to resolve discrepancies. Within 24 hours of the advisory issued by FedCIRC, the CIPM can provide status updates to the DOC CIO and other external authorities as necessary.

Graphic Flow of DOC Significant Incident Coordination and Communication Process for Significant Events